UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/499,633	02/08/2000	Young-Soon Cho	0630-0981P	1525

7590 09/03/2002

Birch Stewart kolasch & Birch LLP
P O Box 747
Falls Church, VA 22040-0747

EXAMINER
LE, DAVID Q

ART UNIT	PAPER NUMBER
3621	

DATE MAILED: 09/03/2002

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/499,633	CHO ET AL.
	Examiner	Art Unit
	David Q Le	3621

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____ .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-14* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-14* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☒ Certified copies of the priority documents have been received in Application No. *09/499,633* .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) do not apply to the examination of this application as the application being examined was not (1) filed on or after November 29, 2000, or (2) voluntarily published under 35 U.S.C. 122(b). Therefore, this application is examined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

2. **Claim 1** is rejected under 35 U.S.C. 102(e) as being anticipated by **Schneck et al**, US Patent No 5,933,498, issued Aug 3, 1999 and filed on Nov 5, 1997.

Schneck describes an apparatus for controlling access to digital data (Fig 1; Col 7, lines 8-55) with features and functionalities that meet all the limitations of claim 1:

> *an apparatus for decrypting an encrypted digital data file* (Schneck's "access mechanism"), *comprising:*
>
> *a digital data playing device for receiving the encrypted digital data file, storing the encrypted digital data file in a data storage medium, and decrypting the stored digital data file using an encryption key* (Fig 8; Col 15, lines 19-38; Figs 9-12), *wherein*
>
> *the encryption key is generated on the basis of an identification number of the data storage medium or an identification number of the digital data playing device* (Col 14, lines 32-50).

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. **Claims 2-14** are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneck.

As per **claim 2**:

Schneck discloses that data distributed via his system may be protected by encrypting the data with a "data-encrypting key K_D". This K_D may be the same for all copies of the packaged data. This K_D may be further encrypted by a "rules-encrypting key K_R", wherein K_R is unique to each version of the system or each receiving player/computer of each user (Fig 4; Col 12, lines 1-16). Schneck further discloses that the algorithms used in the generation and application of said encrypting keys may be selected from many established encryption algorithms, depending on the assessment of risks and degree of protection of the data desired (Col 12, lines 27-48). Additionally, Schneck discloses that the serial number of a device may be used in the generation of his rules-encrypting key K_R (Col 14, lines 31-50).

Schneck does not specifically disclose that information regarding a manufacturing company should be included in the encryption key used to encrypt the data.

However, Schneck teaches that effective protection of the data may be accomplished by encrypting the data and rules governing its access using various combinations of encryption keys, one of which may be specific to the intended user or device used to access the data.

Therefore it would have been obvious for one ordinarily skilled in the art at the time the invention was made to have applied Schneck's teaching to create an apparatus wherein

the encryption key includes information regarding a manufacturing company and a serial number of the data storage medium or the digital data playing device (i.e. Schneck's K_R).

Such an embodiment would meet the limitations of claim 2, and would have been motivated by a desire to very specifically control access to data being distributed, according to each specific user or class of user (each user having bought a player device from a specific manufacturer, each such player uniquely identified by its serial number).

As per **claim 3**:

As the references cited per claim 2 show, Schneck discloses that encryption keys used in his system may be derived using many different, well known encryption algorithms. Using additional arbitrary values in such encryption algorithms (i.e. semi-random or random numbers) is well known within the art. Therefore it would have been obvious to one ordinarily skilled in the art at the time the invention was made that a system could have been set up with

the apparatus as set forth in claim 2, wherein the encryption key further includes an arbitrarily set value,

for the purpose of making the transmitted encrypted data harder to crack thus better protected.

As per **claim 4**:

Schneck discloses that the playing device in his system may be configured so that all data is protected by encryption within an "access mechanism" (Figs 8, 9, 10b, 11; Col 15, line 19 – Col 17, line 33).

Therefore it would have been obvious to one ordinarily skilled in the art at the time the invention was made to have set up an apparatus

further comprising: a processor for decrypting a previously encrypted digital data file and reproducing the digital data file, or re-encrypting the decrypted digital data file using the encryption key and transmitting the re-encrypted digital data file to the digital data playing device.

This would have been done to further protect the data from being misused or illegally intercepted, copied, or transmitted at the user's end. Even when being transmitted from a processor that received the data to a playing device, the data would be encrypted and thus protected.

As per **claim 5**:

In view of the Schneck references used per claims 1 and 2 above, it would have been obvious for one ordinarily skilled in the art at the time the invention was made to devise a method meeting the limitations of claim 5, namely:

a method for encrypting or decrypting a digital data file, comprising adding a first internal key to an identification number of a digital data player or an identification number of a data storage medium associated therewith, thereby generating a first encryption key; and encrypting or decrypting the digital data file based on the first encryption key.

Such a method would have been motivated by the desire to encrypt protected data based on (1) the nature of the data itself and (2) the specific access privileges granted to individual users or the devices they'll use for accessing the data.

As per **claim 6**:

Similarly, using Schneck's teachings as cited above, it would have been obvious for one ordinarily skilled in the art at the time the invention was made to have devised

the method as set forth in claim 5, further comprising: encrypting the first encryption key using a second internal key to produce a second encryption key, wherein the encrypting or decrypting step includes encrypting or decrypting the digital data file using the second encryption key.

This method would have been devised to further protect the integrity/safety of the key used in decrypting the data itself. In this fashion, first the data key would have to be decrypted using the second encrypting key, then the data itself may be decrypted using the data key. Such a method would result in a much stronger protection for the transmitted data and its access rules.

As per **claim 7**:

Schneck discloses that data and rules governing the access to the data may be presented in any order, or in an interleaved fashion (Col 13, lines 54-63), and that packaged data may vary widely and be transmitted to users as single packaged entities or as continuous streams of data, along with appropriate access rules and decrypting keys (Col 15, lines 9-13). Schneck teaches that data and the controls to its access may vary widely, and that the transmission and protection of this data would have to be set up according to many differing parameters, based on the nature of the data, how many discrete parts it consists of, and what access controls apply to each such part.

It would have been obvious to one ordinarily skilled in the art at the time the invention was made to apply Schneck's teachings to devise a method to safely and effectively deliver and control data with multiple usable parts. Such a method would utilize a plurality of keys to control each such part of the data, and as such, would meet the limitations cited in claim 7:

the method as set forth in claim 5, wherein the adding step includes adding a plurality of internal keys to the identification number of a digital data player or the identification number of a data storage medium associated therewith.

As per **claim 8**:

In view of the same Schneck references cited as per claim 4 above, claim 8 is rejected:

the method as set forth in claim 6, wherein the encrypting or decrypting step includes decrypting the digital data file using the second encryption key in a digital data playing device.

As per **claim 9**:

In view of the same Schneck references cited as per claim 4 above, claim 9 is rejected:

the method as set forth in claim 8, further comprising: encrypting raw data in a processor using the second encryption key to generate the digital data file; and transferring the digital data file to the digital data playing device

As per **claims 10-14**:

Claims 10-14 are rejected in view of the Schneck references cited above for claims 1-9. A program embodied on computer-readable medium would have been inherent in a system, method and apparatus configured as specified in the above claims and would have met the limitations cited in claims 10-14:

10.A program (or script) embodied on a computer-readable medium for encrypting or decrypting a digital data file, the computer-readable-medium-embodied program comprising:
a first program code segment to input an identification number of a digital data player or a data storage medium associated with the digital data player;
a second program code segment to add a first internal key to the inputted identification number to convert the identification number into a first encryption key; and
a third program code segment to encrypt or decrypt a digital data file based on the first encryption key.

11.The program as set forth in claim 10, further comprising: a fourth program code segment to encrypt the first encryption key according to an encryption algorithm using a second internal key, wherein
the third program code segment encrypts or decrypts the digital data file using the encrypted first encryption key.

12.The program as set forth in claim 11, wherein the third program code segment encrypts the digital data file.

13. The program as set forth in claim 12, wherein the fourth program code segment is substantially the same as the third program code segment.

14. The program as set forth in claim 11, wherein the third program code segment decrypts the digital data file.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to David Q Le whose telephone number is 703-305-4567. The examiner can normally be reached on 8:30am-5:30pm Mo-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James P Trammell can be reached on 703-305-9768. The fax phone numbers for the organization where this application or proceeding is assigned are 703-305-7687 for regular communications and 703-305-7687 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-308-1113.

DQL
August 26, 2002

JAMES P. TRAMMELL
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 3600